

1 L. KIERAN KIECKHEFER, SBN 251978
kkieckhefer@gibsondunn.com
2 JOSEPH A. GORMAN, SBN 267553
jgorman@gibsondunn.com
3 CHRISTINA MYROLD, SBN 324183
cmyrold@gibsondunn.com
4 GIBSON, DUNN & CRUTCHER LLP
One Embarcadero Center, Suite 2600
5 San Francisco, CA 94111-3715
Telephone: 415.393.8200
6 Facsimile: 415.393.8306

7 ILISSA SAMPLIN, SBN 314018
isamplin@gibsondunn.com
8 GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
9 Los Angeles, California 90071-3197
Telephone: 213.229.7000
10 Facsimile: 213.229.7520

11 AHMED ELDESSOUKI, *pro hac vice*
aeldessouki@gibsondunn.com
12 GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
13 New York, NY 10166-0193
Telephone: 212.351.4000
14 Facsimile: 212.351.4035

15 *Attorneys for Plaintiff*
16 *CADENCE DESIGN SYSTEMS, INC.*

17 **IN THE UNITED STATES DISTRICT COURT**
18 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**
19 **SAN JOSE DIVISION**

20 CADENCE DESIGN SYSTEMS, INC., a
21 Delaware corporation,

22 Plaintiff,

23 v.

24 JEFFREY APPLEBAUM,

25 Defendant.
26
27
28

Case No.: 5:24-cv-00290-PCP

**STIPULATION AND [PROPOSED]
ORDER REGARDING PROTOCOL FOR
FORENSIC INSPECTION OF
DEFENDANT'S DEVICES AND
ACCOUNTS**

1 Plaintiff Cadence Design System, Inc. (“Cadence”) and Defendant Jeffrey Applebaum
 2 (collectively, the “Parties” and individually, a “Party”), by and through their respective counsel of
 3 record, hereby stipulate and agree as follows:

4 WHEREAS, on January 16, 2024, Cadence filed a motion for a temporary restraining order
 5 against Mr. Applebaum, alleging misappropriation of trade secrets and breach of contract;

6 WHEREAS, on January 23, 2024, the Court ordered Mr. Applebaum “to turn over all devices
 7 by 5:00 PM on Friday, January 26, 2024” for forensic imaging and analysis, and further ordered the
 8 parties to “file a proposed order re timeline and protocol by 5:00 PM on Wednesday, January 31, 2024”
 9 (D.I. 23);

10 WHEREAS, on January 24 and January 25, 2024, FTI Consulting Technology LLC (“FTI”)
 11 acting as the forensic vendor for this matter collected electronic data sources from Mr. Applebaum, all
 12 of which have been returned to Mr. Applebaum or his counsel on or before January 29, 2024;

13 WHEREAS, the parties have met and conferred through their respective counsel of record, and,
 14 subject to the Court’s approval, HEREBY STIPULATE AND AGREE AS FOLLOWS:

15 **1. PURPOSES AND LIMITATIONS**

16 **1.1** The Parties have agreed to conduct collection, imaging, and document and forensic
 17 review of the contents of Mr. Applebaum’s devices and accounts to identify any
 18 confidential, propriety, and/or trade secret information of Cadence in Mr. Applebaum’s
 19 possession, custody, or control. The protocol described in this Order (the “Protocol”)
 20 does not waive or prejudice any Party’s right or entitlement to take discovery from any
 21 other repository or data source.

22 **2. DEVICES AND REPOSITORIES SUBJECT TO THIS PROTOCOL**

23 **2.1** The electronic devices and storage repositories subject to this protocol include:

- 24 1) all electronic computing and storage devices (e.g., desktop computers, laptop
 25 computers, tablets such as Apple iPads, mobile telephones such as Apple iPhones,
 26 USB drives, external hard drives, CD/DVD/Blu-Ray discs, etc.) that Mr.
 27 Applebaum represented were, are, or have been used or accessed by Mr.

Applebaum at any point during the period between March 2006 and ending January 23, 2024 (“Timeframe”) that remain in his possession, custody, or control, including all personal as well as Cadence-issued devices, but excluding any devices issued to Mr. Applebaum by his current employer (collectively, “Physical Devices”); and

- 2) all electronic mail, storage, instant message, or other accounts or repositories capable of storing electronic information (e.g., email accounts (e.g., Gmail, Yahoo!, etc.); electronic storage accounts (Dropbox, Box, OneDrive, etc.); electronic information repositories (OneNote, Evernote, Notion, etc.); and omnibus accounts capable of email and/or electronic storage (Apple, Google, etc.), that were, are, or have been used or accessed by Mr. Applebaum at any point during the Timeframe that remain in his possession, custody, or control, including all personal as well as company-issued accounts or repositories, but excluding any accounts or repositories to which access was granted to Mr. Applebaum by his current employer (collectively, “Cloud Accounts” and, along with Physical Devices, the “Data Sources”).

3. PROTOCOL FOR FORENSIC INSPECTION AND PRODUCTION

3.1 *Forensic Vendor.* Cadence has engaged FTI as a third-party forensic analyst and expert to conduct collection, imaging, and document and forensic review of the Data Sources. FTI agrees to be bound by the terms of this Protocol.

3.2 *Tendering of Devices & Repositories to Forensic Vendor.* To the extent not previously tendered, Mr. Applebaum shall tender to FTI, in accordance with FTI’s reasonable collection policy, all remaining Data Sources for preservation through forensic capturing. Mr. Applebaum shall also provide FTI with any necessary login IDs, passwords, encryption keys, two-factor authentication information, or other information required to access the Data Sources.

3.3 Mr. Applebaum shall certify, in a sworn written statement, that he has produced all Data

Sources to FTI for forensic capturing pursuant to this Protocol.

3.4 *Full Forensic Preservation.* FTI will perform full forensic captures (the “Full Forensic Capture”) of each Data Source tendered to it, in accordance with the terms of this Protocol. FTI may perform the Full Forensic Capture prior to the entry of this stipulation by the Court.

3.3.1 Full Forensic Captures shall include all content and user generated data (“User Generated Data”) available for collection.

3.3.2 All Full Forensic Captures shall be preserved, stored, and maintained by FTI until it is destroyed pursuant to the terms of the Stipulated Protective Order in this action.

3.3.3 FTI will endeavor in good faith to complete the Full Forensic Capture of each Physical Device within five (5) business days of the tendering of such device, and will make all efforts to return custody of the device as soon as the Full Forensic Capture is complete.

3.3.4 FTI will endeavor in good faith to complete the Full Forensic Capture of each Cloud Account within five (5) business days of receiving passwords, two-factor authentication information, encryption keys, and any other information necessary for FTI to access the Cloud Account, and will make all efforts to return custody of the account as soon as the Full Forensic Capture is complete.

3.3.6 Mr. Applebaum agrees to cooperate in good faith with FTI to assist with the use, operation, and access of the Data Sources, including but not limited to providing power adapters for non-standard power connectors; and cooperating with FTI as needed, for example to change passwords or provide two-factor authentication information.

3.3.7 The good faith time estimates set forth in Sections 3.3.3 and 3.3.4 assume a reasonable number and storage size of Data Sources, as well as a reasonable number and type of third-party applications installed on each; they also assume

reasonable and timely cooperation from Mr. Applebaum with, for example, passwords, two-factor authentication, etc. The Parties agree and acknowledge that an excessive amount of any of the above, as well as other complications that could occur in the process of creating Full Forensic Captures, could cause the Forensic Capturing process to take longer than estimated notwithstanding FTI's good faith best efforts.

3.4 *Non-Content Forensic Artifacts For Production.* Following entry of this stipulation by the Court, FTI shall then render derivative data sets ("Non-Content Forensic Artifacts") for each of the Full Forensic Captures, for files that are viewed, changed, modified, opened, closed, added, deleted, or otherwise accessed in any way within the Timeframe. FTI shall produce the Non-Content Forensic Artifacts for each Data Source to Cadence and to Mr. Applebaum's counsel.

3.4.1 The Non-Content Forensic Artifacts shall contain a file and system activity reporting generated from Non-Content Forensic Artifacts. The Non-Content Forensic Artifacts shall not contain any user content or User Generated Data.

3.4.2 User Generated Data shall be suppressed or excluded when preparing the Non-Content Forensic Artifacts for each of the Data Sources.

3.4.3 The Parties represent that because the Non-Content Forensic Artifacts do not contain User Generated Data, they therefore cannot be reasonably subject to a claim of privilege, privacy, or work product.

3.5 *Deletion Reports For Production.* Following entry of this stipulation by the Court, FTI shall also produce reports of any deletions identified to have occurred on any Data Source within the Timeframe, and shall provide a copy of such report(s) to Cadence and to Mr. Applebaum's counsel.

4. USER GENERATED DATA

4.1 *Requests For User Generated Data.* In the event that Cadence's review of the Non-Content Forensic Artifacts reveals or otherwise indicates that specific User Generated

1 Data may be relevant or contain potentially relevant information to this dispute,
2 Cadence may request in writing that Mr. Applebaum produce the content or User
3 Generated Data (a “Request”).

4 **4.2** *Scope of Requests.* Requests for User Generated Data may include any files or
5 documents that were previously deleted, but can still be recovered using commercially
6 reasonable means, such that the Request may include not only extant documents and
7 items present on the Data Sources, but also deleted files, documents, or portions thereof
8 that are relevant.

9 **4.3** *Form of Requests.* Each Request shall be presented in writing and contain the following
10 information:

11 **4.3.1** A descriptive identification of the Data Source, including by identification
12 number or assigned common name;

13 **4.3.2** The unique identifier of the forensic artifact that is likely to contain relevant and
14 responsive information, and if the forensic artifact is an electronic document that
15 is a “child” of another electronic document, the unique identifier of the parent
16 document will also be listed;

17 **4.3.3** Where applicable and available, the full file paths of each file/item name likely
18 to contain relevant and responsive information; and

19 **4.3.4** A description for the basis of relevance of the information, including, for
20 example, date said file/item was created, modified, accessed, deleted, or
21 transferred, as well as deletion status, file/item extension, encryption status, and
22 other salient metadata.

23 **4.4** *User Generated Data For Production Without Request.* FTI shall also search the Full
24 Forensic Captures following the application of relevant search terms. A summary of
25 any search hits, along with the underlying files themselves, shall be provided by FTI to
26 counsel for Mr. Applebaum; this production shall be considered a Request for the
27 production of all such files pursuant to Sections 4–5 herein.

1 **4.5** *Review of User Generated Data.* In advance of any production of data to Cadence, Mr.
 2 Applebaum's counsel will be given access to review any and all data identified
 3 according to search terms, for seven (7) business days prior to production to Cadence.
 4 Access to this responsive data will be made via secure online portal or as otherwise
 5 convenient for FTI to provide. Mr. Applebaum's counsel shall create a privilege log of
 6 documents over which a privilege or privacy claim is raised (*see* Section 5, *infra*). Mr.
 7 Applebaum may assist in the review of all data identified according to search terms, but
 8 only under the direct supervision of counsel who will ensure that no data is copied,
 9 photographed, printed, manipulated, or kept by Mr. Applebaum.

10 **4.6** *Time for Response.* Absent any timely challenge or objection, FTI shall produce the
 11 content data pursuant to any Cadence Request after the seven business (7) days
 12 constituting Mr. Applebaum's counsel's opportunity to review the data identified.

13 **5. CHALLENGES AND OBJECTIONS TO REQUESTS**

14 **5.1** *Timing for Challenge or Objection.* Mr. Applebaum may challenge or object to any
 15 Request(s) pursuant to Section 4 (including Section 4.4) within four (4) business days
 16 of Cadence's Request. Any and all challenges and/or objections not raised in writing
 17 within four (4) business days of Cadence's Request shall be deemed waived.

18 **5.2** *Permissible Scope of Challenges and Objections.* Challenges and objections may be
 19 made on the grounds of privilege and/or privacy only.

20 **5.3** *Form of Challenge or Objection.* Any challenge or objection must be in writing and
 21 accompanied with a detailed basis for the challenge/objection and proposed date(s) and
 22 time(s) for counsel to meet-and-confer within three (3) days of the challenge or
 23 objection.

24 **5.4** *Privilege Log.* For each challenge or objection, counsel for Mr. Applebaum must
 25 identify the specific content, documents or items among the requested items that are
 26 subject to a claim of privilege, privacy, or work product by Mr. Applebaum, and must
 27 concurrently produce to Cadence a privilege log setting forth such documents or items
 28

as well as the basis for the claim. All documents or data identified as privileged in a Privilege Log will be removed from the production to Cadence until the privilege and privacy claims are resolved. For the avoidance of doubt, any Privilege Log provided pursuant to this Protocol shall comply with Federal Rule of Civil Procedure 26(b)(5)(A), shall be governed by relevant caselaw relating to the same, and shall contain at least the information set forth in **Schedule A** herein.

5.5 *Disputes.* In the event that there is a dispute between the Parties regarding the discoverability of any item subject to a Request, which dispute cannot be resolved despite a good faith meet-and-confer between the Parties, the Parties agree that they will submit the dispute to the Court for resolution.

5.6 *Privileged Communications.* Any items recovered according to the search terms provided in the Requests that are communications between Mr. Applebaum, on the one hand, and Joel Waelty, on the other hand, will be presumed to be privileged attorney-client communication and not subject to production. Notwithstanding the foregoing, these communications will still be logged in a privilege log for Cadence's review as set forth in Section 5.4, *supra*.

5.7 *Privileges Not Waived.* In the event Cadence learns that FTI has disclosed privileged data to Cadence, Cadence and its counsel agree to notify Mr. Applebaum of what may be a privileged communication, to sequester that data, and to refrain from using or reproducing that data until (a) ten (10) days after Cadence advises Mr. Applebaum of the potentially privileged information, if Mr. Applebaum does not make any objection as set forth herein during that time period; (b) Mr. Applebaum's counsel advises Cadence that the documents are not privileged; or (c) pursuant to the objection procedures set forth herein, if Mr. Applebaum makes such an objection during the 10-day period after Cadence advises Mr. Applebaum of the potentially privileged information. Inadvertence in the administration of these protocols will not be deemed to be a waiver.

1 **6. CONFIDENTIALITY DESIGNATION**

2 **6.1** The Parties agree to initially treat all forensic captures, device and repository content,
3 and User Generated Data as HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES
4 ONLY, subject to any de-designation requests or challenges by either party, pursuant to
5 the terms of the Protective Order to be entered by the Court.

6 **6.2** The Parties agree to initially treat all Non-Content Forensic Artifacts as
7 CONFIDENTIAL, subject to any de-designation requests or challenges by either party,
8 pursuant to the terms of the Protective Order to be entered by the Arbitrator.

9 **7. DATA SECURITY**

10 **7.1** FTI will take all precautions standard within the data security field to ensure that the
11 data collected from Mr. Applebaum’s devices and accounts will be kept securely and
12 beyond unauthorized access. All data responsive will likewise be transferred as
13 encrypted and password protected.

14 **7.2** All files will be maintained by counsel for Mr. Applebaum and Cadence subject to
15 industry-standard data security measures.

16 **IT IS SO STIPULATED.**

17 Dated: January 31, 2024

Respectfully submitted,

18 /s/ L. Kieran Kieckhefer

19 L. Kieran Kieckhefer
20 GIBSON, DUNN & CRUTCHER LLP

21 *Attorneys for PLAINTIFF, CADENCE DESIGN*
22 *SYSTEMS, INC.*

23 /s/ Joel Waelty

24 Joel Waelty

25 *Attorney for DEFENDANT, JEFFREY*
26 *APPLEBAUM*

27 ///

28 ///

1 **IT IS SO ORDERED.**

2
3 Dated: _____, 2024

4 _____
5 The Honorable Casey Pitts
6 UNITED STATES DISTRICT JUDGE
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SCHEDULE A

Information to be included on Privilege Log

1. Unique identification number
2. Privilege claimed
3. Document ID
4. Document Type
5. Custodian
6. Data Source (i.e., device or repository on which the file was found)
7. Filename and extension
8. Full path to file
9. Created Date/Time
10. Modified Date/Time
11. Accessed Date/Time
12. For emails or other communications:
 - a. Sent Date/Time
 - b. From
 - c. To
 - d. CC
 - e. BCC
 - f. Subject

E-FILING ATTESTATION

Pursuant to Local Rule 5-1(i)(3), I, L. Kieran Kieckhefer, hereby attest that concurrence in the filing of this document has been obtained from counsel for Defendant Jeffrey Applebaum.

DATED: January 31, 2024

GIBSON, DUNN & CRUTCHER LLP

By: /s/ L. Kieran Kieckhefer
L. Kieran Kieckhefer